Утечки информации в Республике Беларусь. 2019-2020 годы

Оглавление

Только факты

- ✓ В 2019-2020 годах Экспертно-аналитическим центром InfoWatch зафиксировано **22** случая утечки данных из компаний и государственных органов Белоруссии (Республики Беларусь), опубликованных на русском языке[1].
- ✓ В составе зарегистрированных утечек имеется **13** кейсов, в ходе которых были скомпрометированы[2] более **22,4 тыс.** записей персональных данных и платежной информации.
- ✓ Более **40%** утечек произошли в результате действий внешних нарушителей.
- ✓ **3/4 (75%)** утечек внутреннего характера в РБ стали следствием умышленных действий.
- ✓ Более **59%** утечек в республике произошли по сетевому каналу, более **27% -** через сервисы мгновенных сообщений.
- ✓ В каждом втором случае конфиденциальная информация «утекала» из государственных или муниципальных учреждений.
- ✓ Примерно **1/3** всех выявленных случаев компрометации данных пришлись на умышленные утечки персональных данных белорусских силовиков.

[1] Согласно статье 17 Конституции Республики Беларусь, государственными языками являются белорусский и русский языки. Для данного отчета целенаправленно вёлся мониторинг информационных источников на русском языке. В поле исследования выборочно попадали некоторые источники на белорусском языке, однако отдельных случаев утечек конфиденциальной информации выявлено не было.

[2] Компрометация данных — нарушение состояния защищенности, последствие утечки данных.

Сокращения

GDPR	General Data Protection Regulation (Регламент Евросоюза о персональных данных от 27.04.2016 г., вступил в силу 25.05.2018 г.)
ИБ	Информационная безопасность
ИС	Информационная система
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
РБ	Республика Беларусь
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch провел исследование утечек информации, зарегистрированных в органах власти, государственных организациях и коммерческих компаниях Республики Беларусь в 2019-2020 гг. Интерес к теме утечек данных в этом государстве обусловлен исторической связью с Россией, тесными экономическими и культурными отношениями двух стран.

Согласно закону РБ «Об информации, информатизации и защите информации», обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, осуществляется путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям. Этот закон, принятый в 2008 г., неоднократно дополнялся, в соответствии с новыми реалиями.

Авторы отчета уверены, что результаты исследования будут интересны специалистам в области информационной и экономической безопасности, журналистам, собственникам и высшему менеджменту белорусских и российских компаний, которые оперируют информацией ограниченного доступа (коммерческая, банковская, налоговая тайна, персональные данные), иными ценными информационными активами.

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[3] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов.

В настоящий момент количество записей в базе превышает 19 600.

Исследования ЭАЦ в основном ориентированы на анализ сообщений об утечках данных на английском и русском языках, также используется некоторое количество источников на арабском, немецком, французском, испанском и итальянском языках. Во многом с этим связана большая доля информации о российских утечках, сообщений об утечках из компаний англосаксонских стран и Европы. В целях данного исследования использовались публикации только на русском языке.

В ходе наполнения базы утечек ЭАЦ каждое сообщение об утечке классифицируется по закрытому списку признаков. Каждый признак обладает ограниченной вариативностью. К примеру, при классификации по страновой принадлежности, как было указано выше, каждому сообщению ставится в соответствие один из вариантов (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации).

В базу вносятся:

- текст заголовка и сообщения об утечке,
- ссылка на источник сообщения,
- дата публикации сообщения,
- размер причиненного в результате утечки ущерба[4] (если его оценила сама компания, допустившая утечку, или аналитические агентства),
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- государство (страна),
- сфера деятельности обладателя информации (отрасль)[5],
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[6],
- направление деятельности (коммерческая, некоммерческая),
- субъект[7], непосредственно допустивший утечку.

---

[3] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках по всему миру.

[4] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

[5] Выделяются следующие отрасли (отраслевые группы): банки и финансы, медицина, торговля и HoReCa, высокие технологии (в основном ИТ и телекоммуникационные компании), промышленность и транспорт, госорганы и силовые структуры, образование, муниципальные учреждения, другое.

[6] По предполагаемому количеству персональных компьютеров в компании. Малые – до 50 ПК, средние – от 50 до 500 ПК, крупные – более 500 ПК.

Далее каждое сообщение классифицируется по:

- наличию умысла[8] (если действия лица, допустившего утечку, являются умышленными, утечка классифицируется как умышленная / злонамеренная; в обратном случае как неумышленная / случайная);
- каналу утечки,
- типам данных (относятся ли скомпрометированные сведения к персональным данным, платежной информации, государственной или коммерческой тайне, ноу-хау и т.п.),
- вектору воздействия,
- типу нарушителя.

Все перечисленные признаки (конкретные варианты признаков) вносятся при наличии информации, определяются методом экспертной оценки, носят вероятностный характер, если информация неполная или противоречивая. При невозможности классифицировать сообщение (нельзя выявить вариант признака и отразить в базе, если в сообщении об утечке прямо или косвенно нет указания признака), в соответствующем поле проставляется значение «неизвестно». Иных признаков (категорий для классификации) база утечек ЭАЦ не содержит.

Также базу попадают случаи, когда невозможно установить обладателя скомпрометированной информации, но совершенно точно известно, что утекшая информация не является скомпилированным набором данных на основе других утечек. Такие случаи при добавлении в базу классифицируются по всем известным параметрам.

В базу вносится только количество записей, содержащих ПДн и/или платёжную информацию, т.к. в остальных случаях количественные характеристики обычно отсутствуют.

Важно отметить, что наряду с неквалифицированными «простыми» утечками авторы исследования выделяют «квалифицированные» утечки — случаи, когда деструктивное поведение сотрудников выражается в использовании легитимного (правомерного, санкционированного) доступа к данным в мошеннических целях (манипуляции с платежными данными, инсайдерской информацией); случаи превышения прав доступа, когда сотрудник знакомится, копирует, передает данные, к которым не должен иметь доступа по роду службы или работы. Указанные признаки также устанавливаются на основе экспертной оценки.

В случаях, когда тип нарушителя неизвестен, и удельный вес таких неизвестных в выборке незначителен (как правило, менее 3%), авторы исследования также

---

[7] Авторы классифицируют утечки по виновнику инцидента. Используются следующие категории: внешний нарушитель - хакер/неизвестное лицо, рядовой сотрудник, топ-менеджер (руководитель), системный администратор, подрядчик: сторонний исполнитель работ по заказу компании, партнер и внештатный сотрудник; бывший сотрудник. См. Глоссарий.

[8] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия вины в действиях лица, которые привели к утечке данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы. См. Глоссарий.

добавляют их к внешним нарушителям, т.к. подобная выборка соответствует данным, полученным при изучении аналогичных случаев.

Сообщения об утечках (единицы совокупности или элементы выборки) в базе ЭАЦ далее именуются утечками. Т.е. каждая запись в базе ЭАЦ содержит сведения об одном событии, которое полностью соответствует приведенному выше определению утечки данных (информации).

Авторы считают, что большие шансы стать известными имеют случаи утечки данных, ставшие следствием:

- кражи в целях продажи неопределенному кругу лиц;
- действий хактивистов для достижения общественных и политических целей;

а также утечки из наиболее крупных и широко известных компаний, организаций, учреждений.

Кроме того, крупные утечки (объемом более 1 млн записей) и утечки из компаний с известными брендами чаще попадают в сферу внимания СМИ, блогеров, надзорных органов. Для анализа и корректного расчета среднего числа записей в одной публичной утечке выделена отдельная категория - «мега-утечка», то есть утечка, в результате которой было скомпрометировано 10 млн и более записей. Отдельно могут исследоваться и все утечки с числом скомпрометированных записей от 1 млн, а также вся совокупность утечек с числом записей до 1 млн.

Сведения об утечках представлены с использованием исторических данных — количественных показателей предыдущих лет.

Для повышения качества выводов использованы следующие подходы: исследования проводятся ежегодно на основе выборки, сформированной по единой методике (случайный поиск исходных сообщений об утечках, классификация сообщений по единому списку признаков). При формировании выводов авторы опираются на динамические показатели. Все данные в сравнительных исследованиях (сравнения с аналогичными показателями предыдущего периода) представляются в процентном виде. Исключение: сведения о совокупном количестве утечек, включенных в базу ЭАЦ, объеме записей, скомпрометированных в результате этих утечек, объеме скомпрометированных записей в расчете на одну утечку (только ПДн и платежная информация).

Указанные данные носят иллюстративный характер, дают представление, например, об изменении объемов определенных типов данных, хранимых и обрабатываемых обладателями информации.

В абсолютных показателях также представлены данные в виде так называемой «отраслевой карты утечек» — карта показывает фактическое распределение объема скомпрометированных персональных данных по отраслям (наглядно показывает зависимость объема ПДн в отрасли от размера компании-обладателя информации, числа утечек ПДн).

При анализе выборки по определенному признаку и построении сравнительных диаграмм (такие диаграммы авторы именуют разрезами или распределениями) все

утечки, классифицированные по исследуемому признаку как «неизвестные» и с долей менее 5%, исключаются из выборки, после чего совокупность оставшихся утечек принимается за 100% для распределения по вариантам выбранного признака и последующего представления в диаграммах.[9] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) более ярко, т.е. решает исключительно презентационные задачи. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, представляются отдельные диаграммы.

[9] Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

Результаты исследования

В 2019-2020 гг. Экспертно-аналитическим центром InfoWatch зарегистрировано 22 случая утечки информации ограниченного доступа из коммерческих компаний, некоммерческих организаций, государственных органов и других организаций Белоруссии (Республики Беларусь, РБ). Крупных утечек (с миллионами утекших записей) за этот период времени не выявлено. В результате инцидентов, попавших в поле исследования, в общей сложности скомпрометировано 24,4 тыс. записей персональных данных. Всего зарегистрировано 13 утечек ПДн (59,1% от общего количества). Соответственно, в результате одной утечки ПДн в среднем было скомпрометировано порядка 1700 записей. В результате самого крупного инцидента «утекло» более 22 тыс. записей.

> *Tgstat.ru/Утечки информации: В свободном доступе в Сети появилась база данных белорусской страховой компании «Белгосстрах». В Excel-файле находились 22 тыс. строк персональных данных, включающие номер карты, ФИО, пол, телефон, адрес и дату рождения.*
>
> *Белсат: В МВД Республики Беларусь сообщили о выявлении случаев утечек информации из милицейских сводок. В частности, обнародованы сведения о происшествиях с участием личного состава. Министр отметил, что к утечке могли быть причастны сотрудники министерства.*

За рассматриваемый временной период более 40% утечек в РБ произошли по вине внешних нарушителей (см. Рисунок 1). При этом в 2020 г. эта доля составила около 54%.

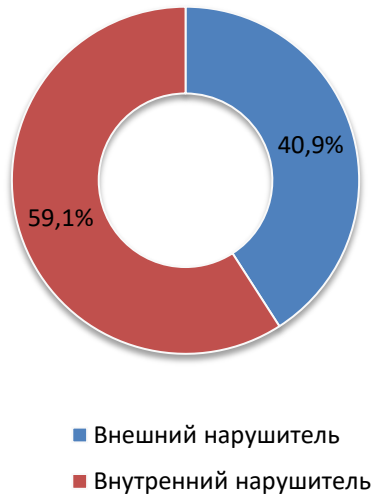

Рисунок 1. Распределение утечек по вектору воздействия в Белоруссии, общее за 2019-2020 гг.

> *Афиша Daily: В Telegram появился канал «Террористы Беларуси», где публикуют, предположительно, личные данные белорусских силовиков, участвующих в подавлении протестов. Авторы уточняют, что на канале появляются данные*

только сотрудников ОМОН. Администраторы приводят имена и номера телефонов предполагаемых силовиков, а также ссылки на их страницы в соцсетях.

Рост доли утечек, вызванных внешними факторами, обусловлен политической ситуацией в Республике Беларусь. После оглашения предварительных итогов президентских выборов, состоявшихся 9 августа 2020 г., в стране начались массовые акции протеста. Противостояние властей и оппозиции вылилось в подавление ряда митингов. В результате протестующие, используя свои каналы, начали «сливать» в Интернет данные силовиков.

> *Reuters: На фоне протестов анонимные хакеры слили в Сеть личные данные более 2000 сотрудников органов внутренних дел в ответ на репрессивные действия, в ходе которых были задержаны тысячи людей. Многие протестующие жаловались на избиения и пытки в тюрьмах.*

В ответ на компрометацию данных силовиков в МВД республики заявили, что располагают необходимыми технологиями для привлечения к ответственности подавляющего большинства виновных в утечке персональных данных правоохранителей.

> *Белтелерадиокомпания: Оперативники ГУБОП в ноябре задержали 35-летнего инженера телекоммуникационной компании, который имел доступ к паспортным сведениям, а также адресам и номерам телефонов абонентов. За два месяца мужчина по заказу незнакомого человека передал данные 60 правоохранителей. В последующем эта личная информация появилась в деструктивных Телеграм-каналах.*

На Рисунке 2 представим соотношение утечек внутреннего и внешнего характера отдельно за 2019 и 2020 годы.

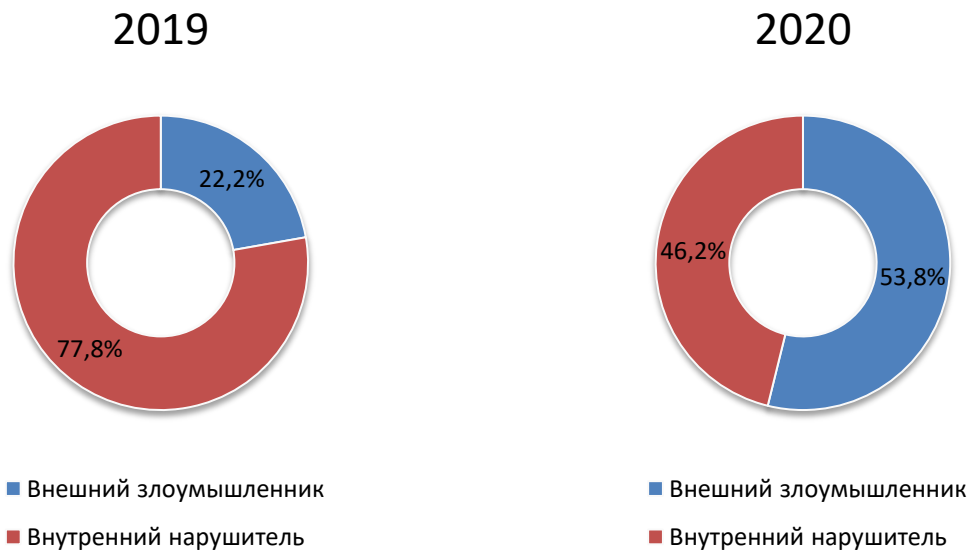

Рисунок 2. Распределение утечек по вектору воздействия в Белоруссии, отдельно за 2019 и 2020 год

Здесь можно отметить, что и общий рост числа зарегистрированных утечек в РБ за 2020 год – более чем на 44% по сравнению с 2019 годом – вызван накалившейся политической обстановкой, когда компрометация данных использовалась оппозицией как средство борьбы с действующей властью.

На Рисунке 3 представлено распределение утечек 2020 г. по месяцам. После относительного затишья в первой половине года отмечен всплеск числа зарегистрированных утечек в конце лета-начале осени, когда в Беларуси произошло обострение борьбы на политическом поле. В результате 77% утечек 2020 года были зарегистрированы в его второй половине.

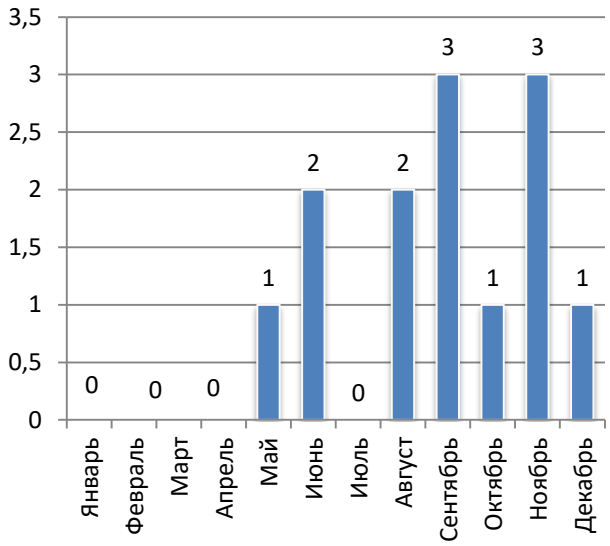

Рисунок 3. Распределение утечек 2020 года в Белоруссии по месяцам

Большинство утечек в Белоруссии за последние два года произошли по вине различных категорий внутренних нарушителей (см. Рисунок). Каждая вторая утечка связана с действиями рядовых сотрудников.

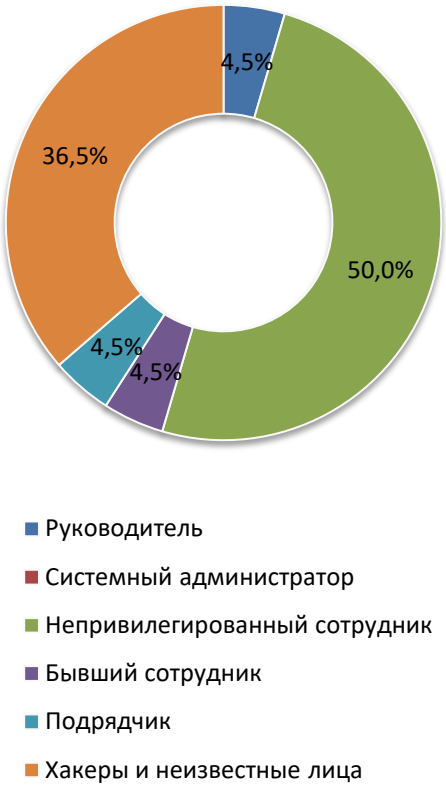

Рисунок 4. Распределение утечек по виновникам в Белоруссии, 2019-2020 гг.

> *Белта: В городе Борисов сотрудница одного из банков, имея доступ к персональным данным, через мобильное приложение оформляла кредитные договоры на имя клиентов и затем распоряжалась деньгами по своему усмотрению. Ущерб составил более 40 тыс. белорусских рублей (примерно $16 тыс.).*

Только 25% утечек внутреннего характера в Республике Беларусь носили случайный характер. Соответственно, три четверти инцидентов были связаны с умышленными действиями персонала (Рисунок 5). Вероятно, это свидетельствует о назревшей проблеме более широкого внедрения средств защиты информации в корпоративном периметре, в том числе систем предотвращения утечек. Судя по всему, внутренние нарушители в белорусских компаниях и госорганизациях уже почувствовали «вкус к данным», то есть возможность извлечения прибыли из доверенной им работодателями информации.

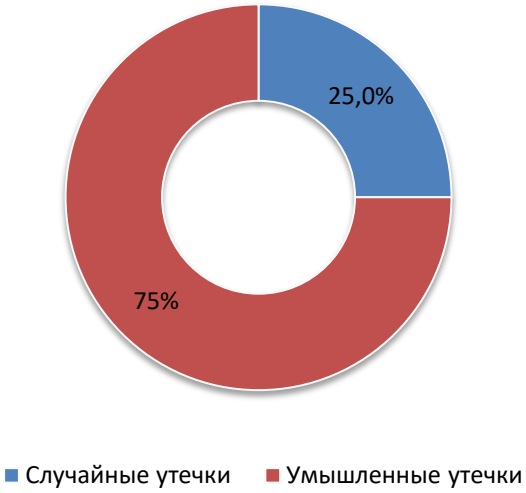

Рисунок 5. Распределение утечек внутреннего характера в Белоруссии по умыслу, 2019-2020 гг.

Более 86% утечек в Белоруссии за 2019-2020 гг. произошли через Сеть и сервисы отправки мгновенных сообщений (Рисунок 6). При этом не было зарегистрировано утечек через такие некогда распространенные каналы, как электронная почта, оборудование и бумажные документы.

Возвращаясь к теме утечек, вызванных обострением политической ситуации, отметим, что большинство из них произошли через мессенджеры. После августа 2020 г. данные белорусских силовиков утекали, судя по опубликованным данным, по инициативе внешних нарушителей. При этом во многих случаях вектор мог быть гибридным: оппозиция «добывала» данные правоохранителей не только в результате взломов информационных систем и использования открытых источников, администраторы некоторых Telegram-каналов и других площадок могли иметь информаторов в силовых структурах их числа сочувствующих протесту, которые имели возможность как напрямую передавать данные, так и помогать реализовывать внешние атаки. Еще в 2019 г. в МВД республики официально признавали факты утечек, к которым могли быть причастны сотрудники министерства.

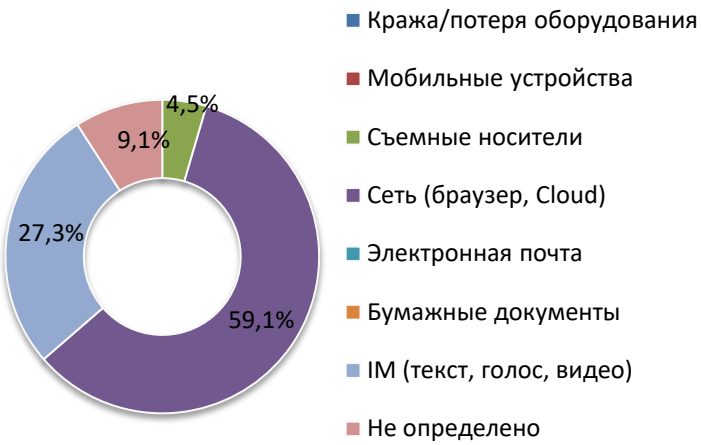

Рисунок 3. Распределение утечек по каналам в Белоруссии, 2019-2020 гг.

Белсат: В МВД Республики Беларусь сообщили о выявлении в 2019 году случаев утечек информации из милицейских сводок. В частности, обнародованы сведения о происшествиях с участием личного состава. Министр отметил, что к утечке могли быть причастны сотрудники министерства.

Хартия'97: Telegram-канал белорусских «кибер-партизан» добыл личные данные сотрудников следственного изолятора КГБ Белоруссии на улице Окрестина в Минске. Опубликована личная информация 12 руководителей, которые могут быть причастны к пыткам противников власти.

Распределение утечек по типам данных демонстрирует, что без малого 60% инцидентов связаны с компрометаций персональных данных, а примерно каждая пятая утечка в РБ – это случай потери или кражи данных, относящихся к категории «коммерческая тайна» (Рисунок 4).

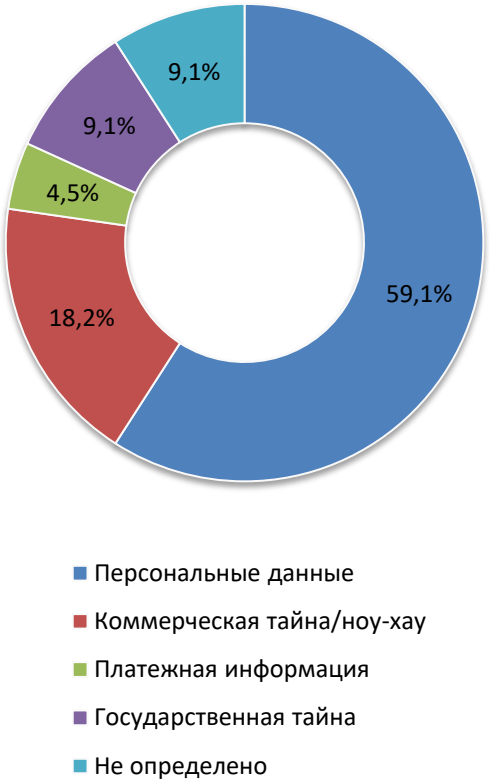

Рисунок 4. Распределение утечек по виновникам в Белоруссии, 2019-2020 гг.

БелНовости: Работая специалистом в одном из филиалов компании сотовой связи, 37-летняя женщина имела доступ к персональным данным клиентов, которые приобретали сим-карты. От имени пользователей она оформляла покупку сотовых телефонов в рассрочку, после чего продавала эти устройства, а деньги присваивала.

Sputnik Беларусь: Бывший сотрудник РУП «Белтаможсервис», используя вредоносные программы, осуществлял несанкционированный доступ и копирование информации из базы данных компании. Информация затем использовалась в интересах ряда коммерческих структур. С ее помощью оценивались риски при осуществлении договорных отношений, устанавливался объем товарооборота предприятий и, что самое важное, проводилась работа по переманиванию крупных клиентов.

Волна утечек, спровоцированных политическими протестами в Республике Беларусь, серьезно повлияла и на отраслевое распределение инцидентов. В результате по итогам 2019-2020 гг. более 45% инцидентов произошли в государственных организациях и силовых структурах (см. Рисунок 7).

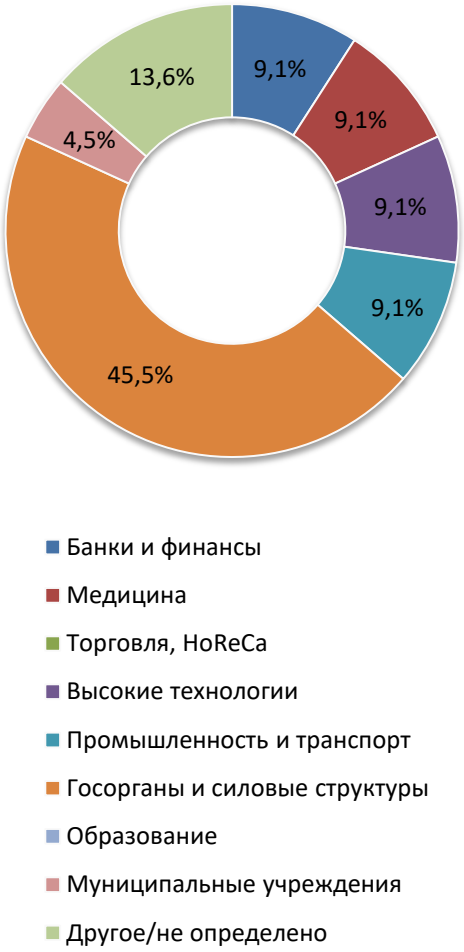

Рисунок 5. Отраслевое распределение утечек в Белоруссии, 2019-2020 гг.

> SecurityLab.ru: *Хакеры взломали внутреннюю электронную систему отделов принудительного исполнения (аналог российской службы судебных приставов) министерства юстиции Республики Беларусь. Взломщики начали транслировать на компьютеры сотрудников видеоролик политического характера. Хакеры утверждают, что им удалось украсть терабайты данных.*

В период распространения коронавирусной инфекции Республика Беларусь не избежала утечек конфиденциальной информации пациентов с COVID-19 и связанных с ними лиц. К сожалению, такие утечки приводили к дискриминации заболевших и грубому вторжению в их личное пространство (в частную жизнь).

> Naviny.By: *Правозащитники отмечают, что в открытый доступ попали списки адресов проживания зараженных коронавирусом, составленные Гродненским зональным центром гигиены и эпидемиологии. А житель Гродно создал карту с адресами домов, где обнаружены зараженные коронавирусом. Часть из этих адресов относилась к частным одноквартирным домам.*

> Весна: *Женщину, которая работает в сфере здравоохранения, встревожила информация о том, что у двух отдыхающих в местном санатории граждан,*

тест на коронавирус имеет положительный результат. Тогда она попросила, чтобы в местном учреждении здравоохранения ей тоже сделали тест на COVID-19. Спустя несколько дней ей позвонили из санэпидемслужбы и сообщили, что у неё положительный тест на коронавирус. Соответственно, вся семья стала контактом первого уровня, а это её муж и сын. Спустя несколько дней знакомые, друзья и коллеги по работе стали беспокоить семью звонками и расспросами о том, что же произошло. Многие соседи стали пристально следить за жизнью семьи, сообщая в милицию о каждом выходе на улицу. Это привело к тому, что в милицию начали поступать ложные сигналы от соседей на отца и мать.

Заключение

Республика Беларусь – пример того, как в небольшом[10] государстве картина утечек информации может серьезно преломляться под влиянием одного мощного фактора. В данном случае речь идет о ситуации на белорусском политическом поле во второй половине 2020 г. Это послужило катализатором роста числа утечек в республике за 2020 год, прежде всего за счет роста внутренних нарушений.

Однако, рост числа утечек, вызванный противостоянием действующих властей и оппозиции, не должен отвлекать внимание от инцидентов, возникающих в текущей социально-экономической ситуации (хотя и она, безусловно, связана с политикой). Как и в России, в Белоруссии одна из основных проблем в сфере информационной безопасности связана с защитой конфиденциальной информации, прежде всего персональных данных и сведений, составляющих коммерческую тайну, от внутренних нарушителей, стремящихся нажиться на чужой информации в цифровую эпоху. Даже относительно небольшое число выявленных инцидентов – 22 случая за 24 месяца – заставляет задуматься о проблемах с защитой информации в ряде отраслей РБ. Также остаются возможности для повышения уровня «цифровой культуры» граждан республики: как показывают факты, ряд из них готов поступиться чужими правами ради утверждения собственных политических взглядов или с целью получения выгоды.

[10] 94-е место по количеству населения и 84-е по территории в мире

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Атака – см. компьютерная атака, сетевая атака, вторжение.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам [Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России. 3 февраля 2012 г.].

Вектор воздействия – критерий классификации в отношении действий лиц, спровоцировавших утечку (в рамках данного отчета InfoWatch).

Различаются действия внешних нарушителей (нарушителей - хакеров и других лиц, как известных, так и неизвестных) – внешние атаки, направленные против компании, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей, (сотрудники компании и подрядчики, получившие права доступа к ресурсам компании) атакующих системы защиты изнутри (неправомерный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.), а также допускающих утечки данных своими случайными действиями (бездействием).

Внешняя атака – атака, совершенная внешним нарушителем.

Внутренний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Внешний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Деструктивные действия сотрудников – в рамках данного отчета об утечках информации аналитики InfoWatch к таким действиям относят действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, в том числе сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Инцидент – см. инцидент безопасности, инцидент информационной безопасности, компьютерный инцидент.

Инцидент безопасности (Security incident) – неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание – Иногда используется термин ≪несостоявшийся инцидент≫ для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах [ГОСТ 56205-2014, статья 3.2.106]

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р 53114-2008, статья 3.2.7. ГОСТ Р ИСО/МЭК 27001-2006, статья 3.6].

Примечание – Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.
- «Электронная почта» – утечка данных через корпоративную электронную почту.
- «Бумажные документы» – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.

- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].

Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.

В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].

В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и «внутренний нарушитель», а также шесть категорий нарушителей:

- Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.
- Рядовой сотрудник.
- Топ-менеджер (руководитель).
- Системный администратор.
- Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.
- Бывший сотрудник.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.

Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).

В отчетах (исследованиях) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.